CSC-EPL-88/006

2

NATIONAL COMPUTER SECURITY CENTER

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF COMPUTER SECURITY CORPORATION

CITADEL

1 September 1988

Approved for Public Release:
Distribution Unlimited

SUBSYSTEM EVALUATION REPORT

COMPUTER SECURITY CORPORATION

CITADEL

NATIONAL COMPUTER SECURITY CENTER

9800 SAVAGE ROAD

FORT GEORGE G. MEADE MARYLAND 20755-6000

September 1, 1988

FOREWORD

This publication, Computer Security Corporation, Citadel Final Evaluation Report, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Trusted Computer Security Evaluation Center." The purpose of this report is to document the results of the subsystem evaluation of Computer Security Corporation's Citadel product.

Approved:

Eliot Sh September 1, 1988

Eliot Sohmer
Chief, Evaluations, Publications, and Support
National Computer Security Center

ACKNOWLEDGEMENTS

Evaluation Team Members

Caralyn A. Crescenzi
Michael J. Oehler
Randy S. Smith

National Computer Security Center
9800 Savage Road
Fort George G . Meade, Maryland 20755-6000

Further Acknowledgements

The following individuals contributed to the report:

John Wyszynski
John Taylor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Citadel Security product has been evaluated by the National Computer Security Center (NCSC). Citadel is considered to be a sub-system rather than a complete trusted computer system. Therefore, it was evaluated against a relevant subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985. Specifically, the subset for this evaluation included identification & authentication (I&A), discretionary access control, and audit requirements.

The NCSC evaluation team has determined that Citadel, when configured as tested, is capable of providing additional protection mechanisms for the IBM PC/XT and PC/AT.[1] Citadel requires each user to enter a user ID and a valid password in order to gain access to the computer. Citadel maintains discretionary access control by mediating access to files. In addition, Citadel has the capability to audit system activity.

The previously mentioned features must be administrated properly so that Citadel can provide an additional level of trust. This includes restricting access to DOS system files (e.g. COMMAND.COM), programming languages, compilers, Citadel's files, and other utilities. This can be accomplished by protecting these files with Citadel's protection mechanisms and by implementing the menu utility to restrict access to a limited set of programs (see page 3, "Product Overview").

Sub-systems are intended to be implemented on automatic data processing (ADP) systems. Specifically, sub-systems are designed to add a level of assurance to an ADP system that has limited or ineffective security mechanisms. However, sub-systems are not intended to protect any information on an ADP system which processes classified or sensitive information. Nor may sub-systems be added to a trusted system for the sole purpose of processing classified or sensitive information. Sub-systems may not be capable of maintaining the integrity of classified or sensitive information which is required of such systems and they are not to be used as justification for processing classified or sensitive material.

[1] IBM PC/XT and PC/AT are registered trademarks of International Business Machines Corporation.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Managers should note that a sub-system or combination of sub-systems serving various functions may not be capable of protecting classified or sensitive information to the level of assurance required by systems designed for such purposes.. This includes justifying the additional security mechanisms provided by a sub-system so that classified or sensitive information may be processed on the trusted system.

Sub-systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub-system evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List maintained in the Information Systems Security Products and Services Catalog.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

The Citadel system is a microcomputer software product which provides user identification and authentication, discretionary access control and auditing capabilities. In addition, Citadel has the capability to encrypt programs and files for up to twenty-two users. The system administrator has the option to use the Data Encryption Standard (DES) or Citadel's Encryption format. Also, the administrator may change Citadel's pre-defined encryption key, if necessary.

Throughout this report, Central Administrator (CA) and Local Administrator (LA) are used to represent the security administrator accounts. These accounts give administrators access to Citadel's utilities. Furthermore, the CA account has privileges and capabilities beyond that of the LA.

Boot Protection

Computer Security Corporation offers a circuit board which purportedly prohibits access to the hard drive when a user boots from a floppy disk or when Citadel has been removed. This circuit board, an additional product which was included in the evaluated configuration, complements the security features of Citadel.

Menu Utility

Citadel provides a menu utility which allows users to execute a subset of programs available on the PC.

These programs are selected by the administrator so that certain users are unable to execute restricted programs. Additionally, the menu utility allows the administrator to restrict access to DOS, set the default file group and optional department protection (see page 5, "Protecting Files"), and toggle the auto-protect and auto-encrypt options for each user. This utility is one of Citadel's mechanisms used to prohibit execution of programs which may disrupt the protection installed by Citadel.

Evaluation of Functionality

This section includes an overview of Citadel's Identification and Authentication, Discretionary Access Control, and Audit features.

Identification and Authentication

To gain access to the PC, users must first enter a User ID (UID) and then a valid password. An Administrator is responsible for assigning the UIDs, enforcing unique UIDs, and assigning the initial password for each user. The user ID can be any combination of alphanumeric characters and may be a maximum of eight characters.

Passwords are case sensitive and consist of six to eight alphanumeric characters. The administrator can grant individuals the capability to change their own passwords and mandate the length of time that a password remains valid. Although the CA assigns passwords initially, users are required to change their passwords during the first logon session. This assures that only one individual knows the password.

A combination of five illegal UIDs or passwords causes the PC to lock. Before attempting another login, users must either re-boot the PC or power down and then power up.

The CA has the ability to set password expiration time for non-administrative users. This option ensures that users will change their passwords after a set period of time.

Discretionary Access Control

Citadel has the ability to provide access control between subjects (PC users) and objects (files). This access control functions for files on hard, virtual, and floppy disks (see page 15, "Product Configuration"). Specifically, Citadel interrupts disk I/O requests through DOS to determine if the request can be granted. The determination is based upon the identity of the user or the entry in the Resource Allocation Table (RAT). If the user is the CA, access is granted to all files. If the user is the Local Administrator, access is granted to all files except those protected for the CA. If a normal user, then the RAT is accessed to compare the allowed type of access to the attempted one. If successful, Citadel grants access to the desired file. Otherwise, access will be denied and if the option was selected, an entry in the audit log will be created (see page 12, "Audit").

Resource Allocation Table

The RAT consists of sixty-four file groups and eight departments. The CA's file group, EXECUTE, and ENCRYPT are additional attributes which enhance the protection of the file group and departments. An explanation of file groups and departments is given below; EXECUTE and ENCRYPT are explained in the "Protecting Files" section.

Files marked by a file group are protected by Citadel. File groups are intended to protect user files and to prohibit group access, if needed. A file group can protect any number of files. However, a file can only be protected under one file group. The CA's file group is a special file group which prohibits access for all users except the CA.

Departments essentially provide group access and are intended to be assigned to a logical group of files. Departments differ from file groups in that a file can be protected under or marked by maximum of eight departments. A file must also be marked by a file group before departmental protection is possible.

Protecting Files

A file will be protected when it is assigned to a file group, including the CA's file group. Departments, EXECUTE, and ENCRYPT are additional forms of protection which enhance the file group's protection.

File group and departmental protection can only be assigned to a file if the auto protect option is ON or if an administrator uses the protection utility. This utility is also the only way the CA can protect a file under the CA's file group. All files not assigned by either of these methods are unprotected files and can be accessed globally (public object).

EXECUTE and ENCRYPT provide additional protection beyond that of the file group and possible departmental assignment. Files protected by EXECUTE are prohibited from being copied to other storage devices by Citadel. The only access privilege allowed is execute (program) so long as the user has at least read access through a file group or department. Files protected by ENCRYPT can be observed, modified, and executed, if the user is granted access through either a file group or department. However, the file will always remain encrypted on all storage devices, excluding memory, even if copied.

Auto Protection

Citadel provides an "Auto Protection" capability which automatically protects files when they are saved. They will be protected to a default file group and department(s) (if applicable). This capability can be toggled locally by users, globally set by an administrator, or an administrator can force Auto Protection for individual users. These options can be chosen from either the menu utility, the DOS prompt, or set in the AUTOEXEC.BAT file. For this capability to function properly, the user must possess write access to the default file group.

The default protection placed on a file is determined by an administrator. This is done when an administrator creates the data files for each user for the menu utility or when the user changes the default from the DOS prompt. When using the menu utility, a user is not informed of the default. Therefore, it is the user's responsibility to identify these defaults by asking the administrator.

Access Rights

Only an administrator can assign access rights to file groups and departments. For each user, an administrator can assign either read (R), write (W), log (L), none (N), a combination of these rights, or leave the entry blank. Any combination of the previously mentioned access rights is valid except when a contradiction of access rights occurs. Contradictory access rights are as follows:

Combination	Explanation
RW	W includes R.
NW or NR	a contradiction of rights.
N	when assigned to a department.

Citadel's access decision is based upon the following: The CA is given access to all files and the LA can access all files except ones protected by the CA's file group. A blank entry to file groups and departments is the default. A user will be denied access if the entry to a file group or department(s) protecting a file is blank. If a user has access rights to multiple departments protecting a given file and if any of these is W, then the user is granted W access to this file. However, the user's access right assigned to the file group overrides any departmental access right(s) acquired. In addition, if the administrator assigned L access, then the access to the protected file for a user will be logged.

Figure 1 shows the RAT, a public file, the assignment of two files to various file groups and departments, and three users with certain access rights assigned to these files. User 1 has write access to file 1 through file group 1. User 2 has read access to department 1 and none access to file group 2. File 2 has been assigned to both file group 2 and department 1 so, following the hierarchical structure of Citadel's access control, User 2 is not granted access to file 2. User 3 has not been given any access rights. Therefore, he can only access File 3, as can User 1 and 2. Note, that this figure shows that files can only be assigned to a single file group, optionally assigned to departments, and that file group access takes precedence over departments.

Resource Allocation Table (RAT)

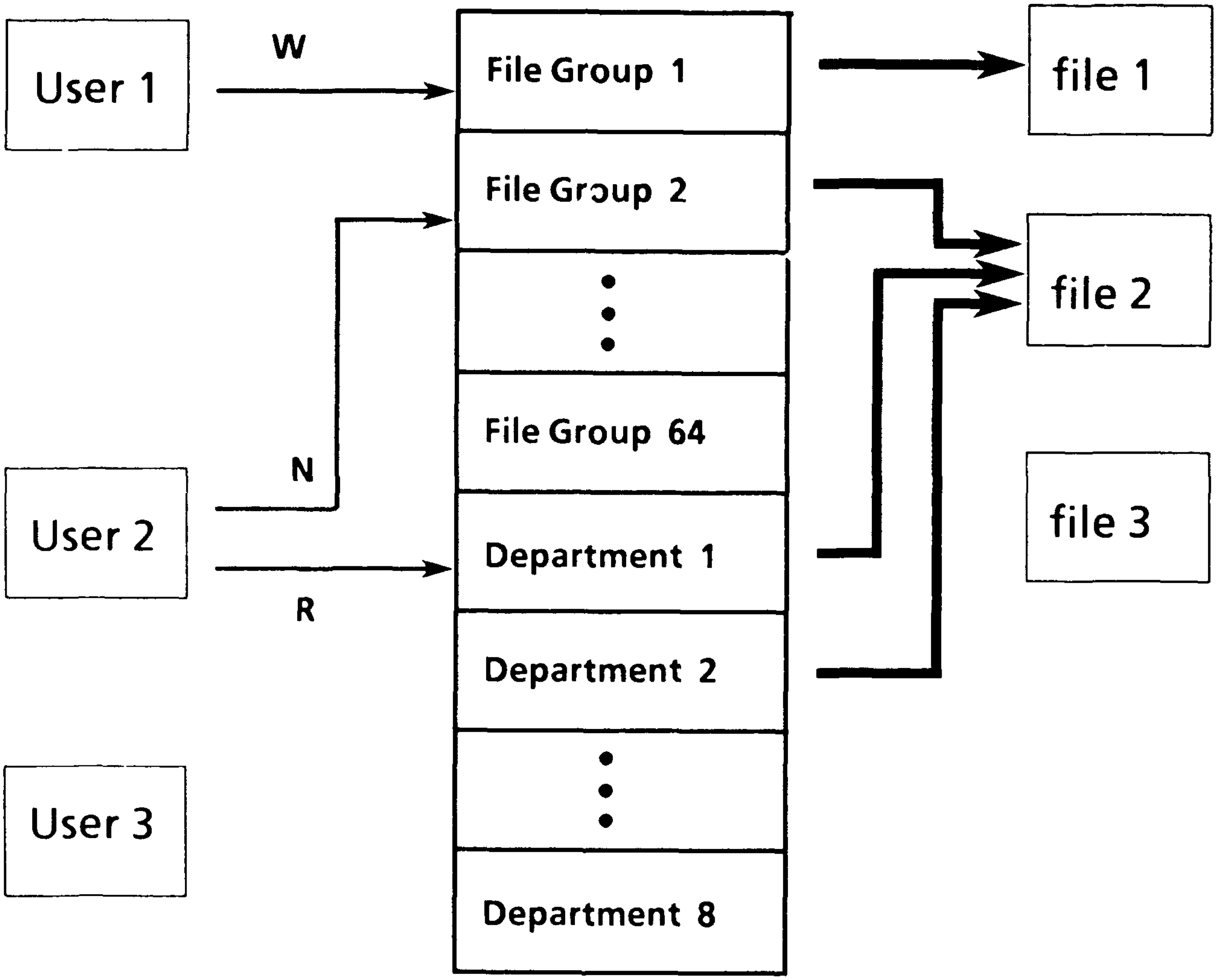

Figure 1

Figure 2 illustrates the RAT, assignment of files to file groups and departments for three files, and the assignment of access rights for three users.

User 1 has read access to any file protected under file group 1. Although User 1 has write access through department 2 to file 2, only read access is given through file group 1. Therefore, File 1 and 2 can be read through this file group. Also note, that file group 1 contains multiple files.

Additionally, User 1 has been assigned write access to file group 2, although there are no files protected by this file group.

User 2 has read and log access to department 2, write access to files in department 3, and log access to files in department 4. When the user tries to access file 2, which is protected under file group 1, department 2, department 3, and department 4, write access will be granted and logged. Therefore when access is granted through multiple departments and multiple access rights are assigned to the departments, W access is given over R, and L access will complement this access.

User 3 has been assigned log access to department 4 and none access to file group 64. When this user tries to access file 3, access will be denied, but not logged because file group access takes precedence over the department. Access to File 2 will be denied and logged because only L access has been assigned to department 4 for user 3 and not R or W.

Note, that file group 3, 63, department 1, and 8 do not have files assigned to them. This does not mean that files can not be assigned to them. It simply illustrates that a file can be protected under any file group or department. Also, both the local and central administrator have full access to any of these files. Lastly, logging occurs regardless of the L access right when the global logging option is set.

Resource Allocation Table (RAT)

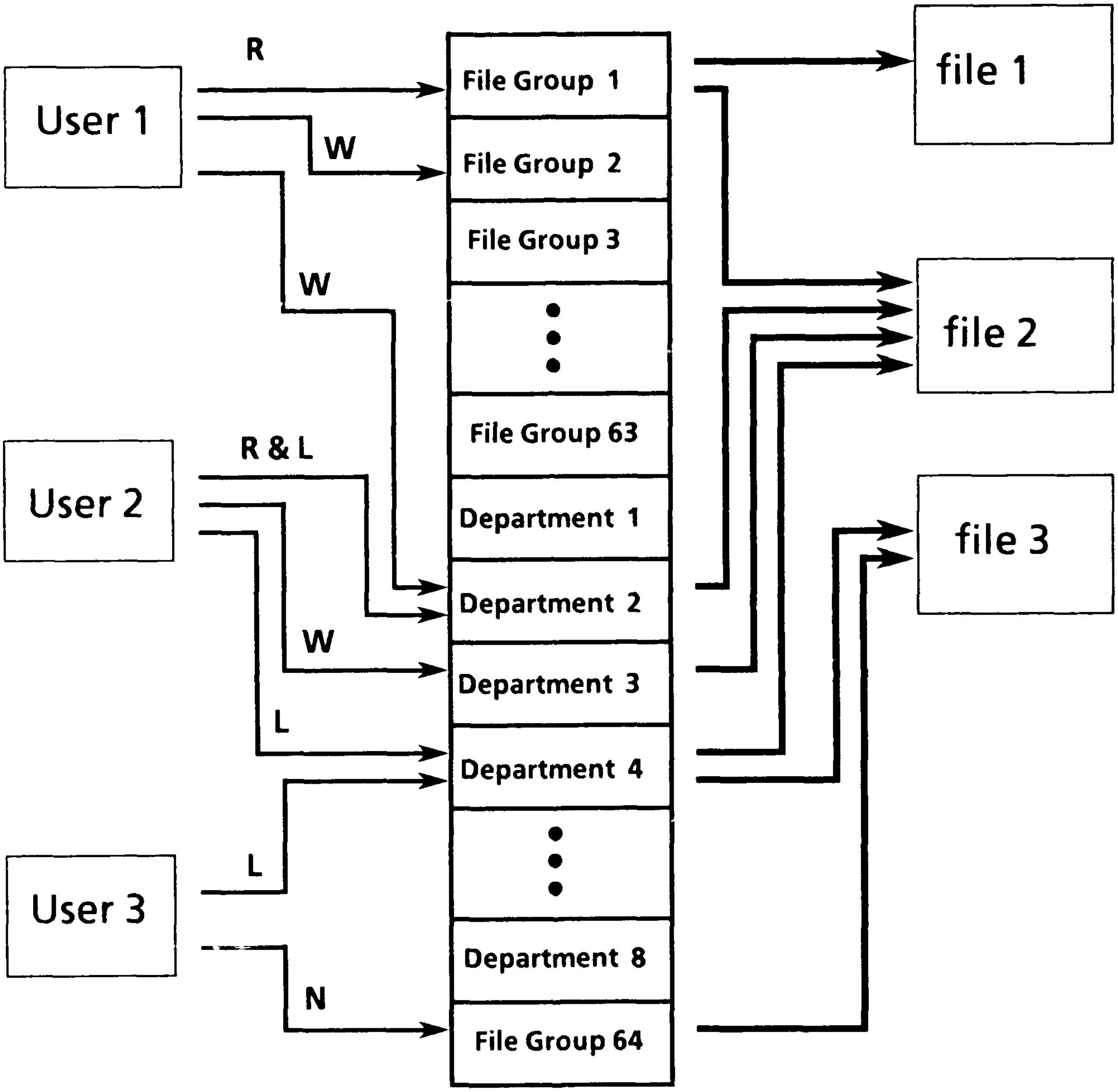

Figure 2

Figure 3 shows the RAT, two users, the CA, protected files, and the additional attributes. EXECUTE has been assigned to ANY.EXE and ANY.COM indicating that it can be assigned to any executable or compiled file. The CA, user 1, and 2 can execute ANY.COM and (except user 2) ANY.EXE. Additionally, ENCRYPT has been assigned to ANY FILE, indicating that it can be assigned to any file. User 2 has read and log access to this permanently encrypted file (the administrators have access also). This figure also shows that the CA's file group protect the central administrator's files and that the CA is the only one with access to them.

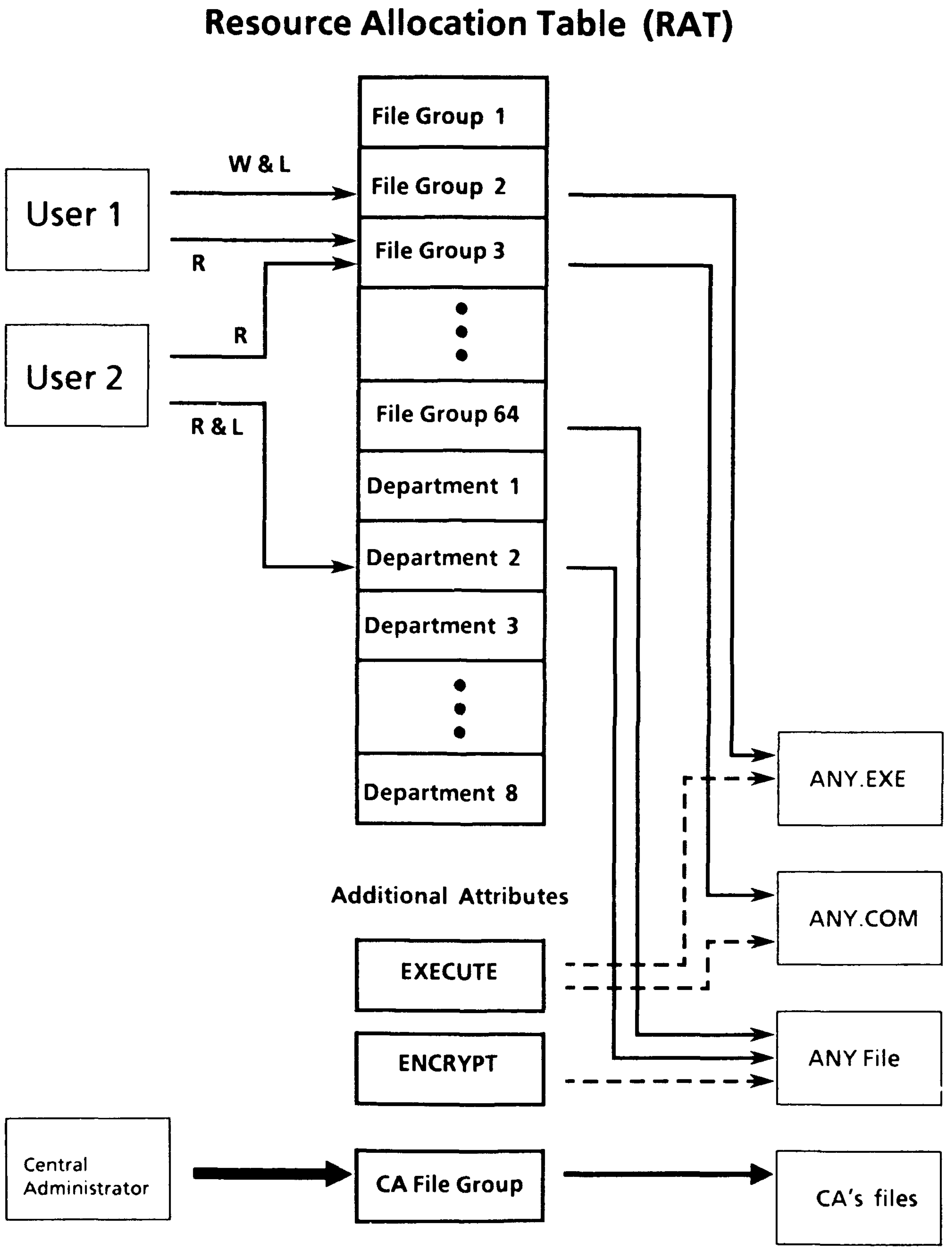
Resource Allocation Table (RAT)
User 1
User 2
W & L
R
R
R & L
File Group 1
File Group 2
File Group 3
File Group 64
Department 1
Department 2
Department 3
Department 8
Additional Attributes
EXECUTE
ENCRYPT
Central Administrator
CA File Group
ANY.EXE
ANY.COM
ANY File
CA's files

Figure 3

Audit

Citadel supplies an administrator with auditing capabilities in order to observe certain specific actions on the system. An administrator can select the following actions: *Time Stamp* (login/logoff), an *Account Number, Log All File Access Attempts, Log All Illegal Access Attempts* to files, and *Changes To Passwords.*

Audit Options

Time Stamp - records the time and date that the user logged in and logged off, along with the unique user number.

Account Number - actually an ASCII string which is recorded in the log. When selected, an administrator selects a maximum string length to control the growth of the log. It is used to keep track of time spent on office projects. Note, this number is not used for I&A purposes.

Log All File Access Attempts - Audits access attempts to protected files.

Log All Illegal Access Attempts - Audits illegal access attempts to protected files.

Changes To Passwords - When a user changes his password, an entry in the audit log will be made.

Audit Report

The administrators can obtain a hard copy of the audit report or display the report on the monitor. The report displays both the audit records of users and a system utilization report.

The audit report of users displays the appropriate audit records that were selected and the user's password. The report displays the time and date of login and logoff, the user name and number, the activity (i.e. illegal access attempt, improper logoff etc.), and the file group name and number associated with that activity. The report also displays the amount of time that the user was logged in at each activity, and the total time logged in.

The system utilization report displays the date, the user name and the time spent on the system. For each day, a daily subtotal and a total time are calculated. The system utilization is figured on this subtotal and total and based on an eight hour work day.

Evaluation of Documentation

The Citadel Security System documentation consists of the following three documents: the Installation Manual, the Administrator Manual, and the User Manual.

The provided documentation thoroughly describes the installation and general implementation of Citadel. However, there are some inconsistencies in the documentation because Computer Security Corporation has added additional features to Citadel which are not reflected in their manuals. Computer Security Corporation intends to update and correct their documentation to accurately describe the capabilities of version 4.0.

Installation Guide

The Installation Guide provides instructions for the system administrator to properly install and remove Citadel. The installation procedure includes how to correctly execute the program, CSCINIT.COM. In addition, this manual explains how to install Citadel on multiple PCs.

Administrator Manual

The Administrator's Manual consists of seven tutorials, a reference section, a message section, and a technical information section.

The tutorials cover the following topics: creating user accounts, installing the menu utility, protecting and encrypting files, and auditing system activity. Each tutorial is divided into several sections which describe the administrative program that carries out the operation.

The reference section describes Citadel commands that can be executed from DOS instead of the menu utility, ENCRYPT only files, EXECUTE only files, and CA files.

The message section explains possible system errors and the actions necessary to correct them.

The technical information section describes the files Citadel uses, software incompatibilities, and Citadel's limitations.

User Manual

The User Manual, intended for general users, describes the procedures for logging on, logging off, changing passwords, and protecting and encrypting files.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data created with these systems. Initially, protection was provided solely by the individuals who maintained physical possession of their own data and operating system on a floppy disk, giving a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users, and thus prevented intentional or accidental access to other users' data . Other security mechanisms were not deemed necessary since users were only able to inflict damage on their own data, or copy of the operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In today's working environment, it is common to have many users share and store their data on the hard disk of a shared microcomputer. In this environment, users no longer have the assurance that their data is protected from unauthorized access, or even that the underlying operating system has not been corrupted.

Citadel, when configured as tested, can provide added security for these types of environments by requiring identification and authentication of users before granting access to the microcomputer, by controlling access to files, and by maintaining an audit trail that specifies the actions of users.

Product Configuration

It was clear that Citadel functioned as claimed. However, since the IBM PC is a single state machine, administrators must effectively control the environment in which Citadel is to be applied. Care must be taken by the administrators when assigning access rights, file groups, and departments for each user and every file. Additionally, proper administrative control must be placed upon the type of executable programs accessible by users and Citadel's additional security features (e.g. floppy boot protection, separation of administrative roles, disabling the PC's break key, and the menu utility). Otherwise, sufficient trust in controlling system resources may be diminished.

The following capabilities were invoked during the configuration and installation of Citadel:

- Auto Protection On

- Menu Utility installed for all users. This included determining the capabilities for each user, restricting DOS access for specific users, selecting programs which used DOS I/O interrupts and ones which could not exit to DOS.

- Hard Disk Lock-out on floppy boot. The software and circuit board which performed this operation were tested separately.

- The device driver to disable the break key was placed in CONFIG.SYS.

- All of Citadel's administrative utilities, CITADEL.COM (the executable part of Citadel), all menu utility files, and AUTOEXEC.BAT were protected so that normal users could not execute or alter them. Citadel's other utilities (library programs) were protected under a file group to which all users had access and under EXECUTE.

Additionally, administrators must ensure that all UIDs are unique, that passwords are managed properly, and that the correct access rights are given to users. Although Citadel is able to distribute its protection capabilities (i.e. file groups and departments) to floppy disks, these files can only be protected if they are used on systems under the control of Citadel.

PRODUCT TESTING

Testing Procedure

The test procedure was intended to demonstrate that the features offered by Citadel functioned as claimed. The team tested Citadel's access control, audit, and identification and authentication mechanisms. Citadel was installed, as described, and user accounts established as per the documentation. The menus and access rights for the users were then carefully defined. Menus were defined such that certain users could not gain DOS access, execute DOS commands, or execute "dangerous" programs (e.g. disk utilities, RAM resident programs, and programs which bypass DOS calls). Access rights were then assigned through file groups and departments to the test files for each user. Citadel was tested on the following systems:

1 IBM PC/XT with 512K main memory DOS 3.2
1 10M hard drive
1 360K 5.25" floppy disk drive
1 Monochrome monitor
1 64K Virtual Disk (RAM Disk)
1 Battery Backup Clock with TIMER program

1 IBM PC/AT with 3M main memory DOS 3.2.
2 30M hard drives
1 1.2M 5.25" floppy disk drive
1 Genius monitor
1 1M Virtual Disk (RAM Disk)
1 Battery Backup Clock

Testing Results

CITADEL Version 4.0 was tested with respect to each of the evaluated security mechanisms.

Identification and Authentication

The logon screen prompted users for their User IDs (UID) and passwords. All entered passwords were not displayed. All illegal log on attempts failed. An illegal attempt consists of five consecutive illegal UIDs and/or passwords. The system audited illegal attempts before locking the PC, as documented. The logon procedure functioned properly.

The option which forces users to change their password after an initial password assignment and after an expiration period function correctly.

After logging on, the menu utility or, if the menu utility was removed, the next command in AUTOEXEC.BAT was executed. If there was no command in AUTOEXEC.BAT, then COMMAND.COM was executed if the user was authorized. This functioned as documented.

The log off program functioned properly. It entered the audit record, if appropriate and returned to the log in screen. It could be executed from the DOS prompt or from within the menu utility. If LOGOUT.EXE was not executed from the root directory, the next user was unable to log in without re-booting the PC.

Additionally, if the user improperly logged off, Citadel did not warn subsequent users, contrary to documentation.

Discretionary Access Control

Citadel's access control performed as documented as long as the precautions mentioned throughout the report and within the documentation were adhered too. This included protection to files on the hard, floppy, and virtual drives.

The assignment of the EXECUTE attribute was not described clearly in the documentat'on and therefore, its proper implementation was difficult.

Audit

Testing of the "log all file access" option revealed that illegal access attempts were not logged. The documentation states that this option, when selected, will log all file access attempts.

The local ability to log all illegal access attempts (L access right) through a file group or department, functioned properly.

A battery backup clock was used to correctly maintain chronological order of the audit log. However, users with DOS access could issue either the TIME or DATE commands to change it and thus, create incorrect audit records.

Additional Features

The Citadel boot protection card and software program used to prohibit access to the hard drive functioned properly.

The disabling of the PC's break key functioned as documented.

Citadel's menu utility functioned effectively. Other administrative utilities functioned as claimed.

The encryption/decryption algorithms were not a part of the sub-system evaluation and therefore not fully considered in testing. However, the team did establish that encrypted data could be successfully decrypted when either the DES or Computer Security Corporation standards was used with the proper keys, respectively. The encryption/decryption test included executable programs, but not COMMAND.COM and AUTOEXEC.BAT.

☆U.S. GOVERNMENT PRINTING OFFICE: 1989 - 622-415/10058

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS None
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; Distribution Unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-88/006	5. MONITORING ORGANIZATION REPORT NUMBER(S) S231,240
6a. NAME OF PERFORMING ORGANIZATION National Computer Security Center 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code)	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE (Include Security Classification) (U) Subsystem Eval Report: Computer Security Corporation Citade	
12. PERSONAL AUTHOR(S) Crescenzi, Caralyn, Oehler, Michael; Smith, Randy	
13a. TYPE OF REPORT Final 13b. TIME COVERED FROM TO	14. DATE OF REPORT (Yr., Mo., Day) 880901 15. PAGE COUNT 28
16. SUPPLEMENTARY NOTATION	
17. COSATI CODES FIELD / GROUP / SUB. GR.	18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Citadel NCSC TCSEC DES CA LA Criteria DAC I&A audit RAT

19. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Citadel system is a microcomputer software product which provides user identification and authentication, discretionary access control, and auditing capabilities In addition, Citadel has the capability to encrypt programs and files for up to twenty-two users. The system administrator has the option to use DES or Citadel's encryption format. Also, the administrator may change Citadel's predefined encryption key, if necessary This report documents the findings of the evaluation

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL DENNIS [illegible]BAUGH	22b. TELEPHONE NUMBER (Include Area Code) (301)859-4458 22c. OFFICE SYMBOL C12

EDITION OF 1 JAN 73 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE